FIG. 1

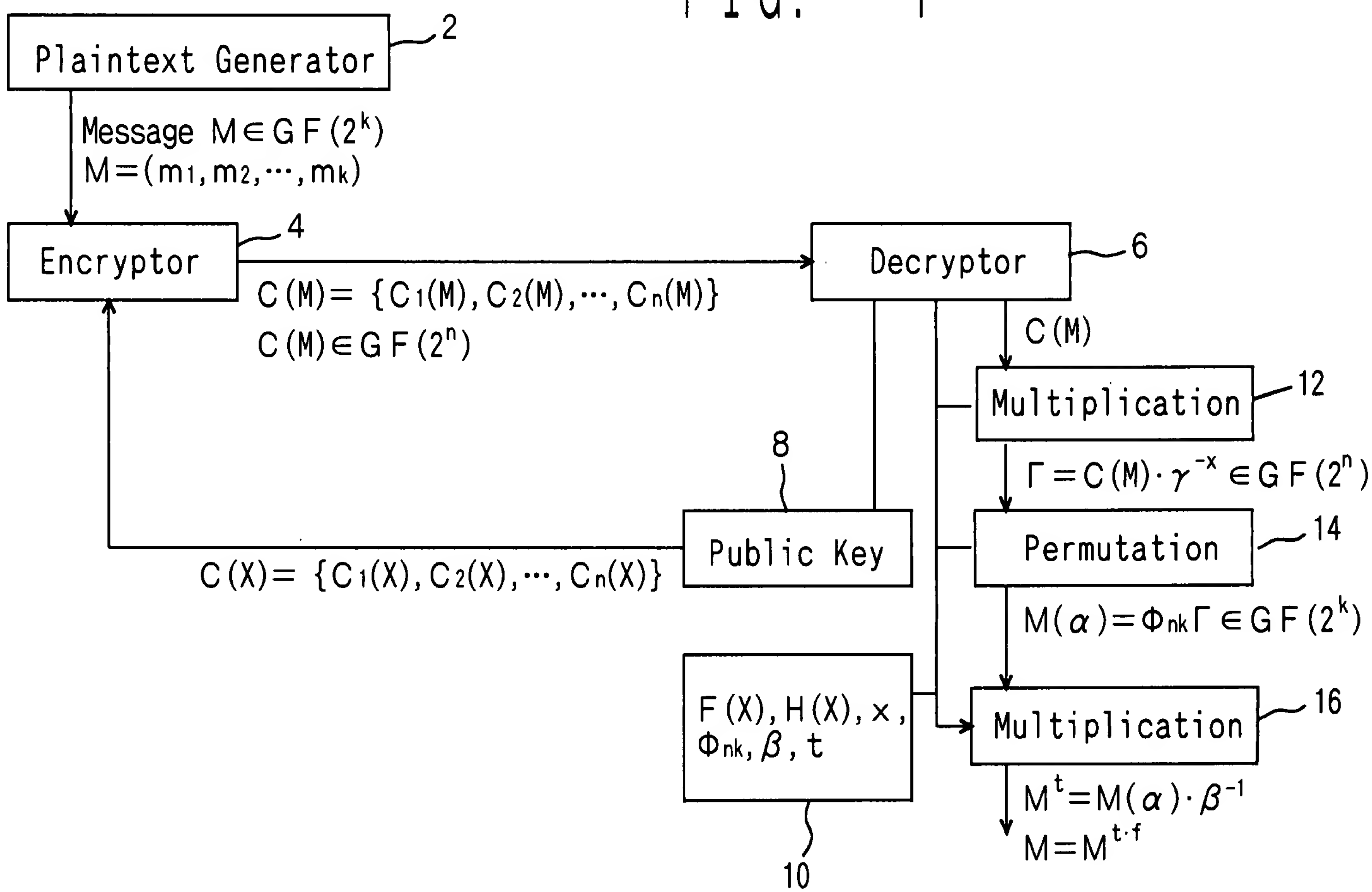
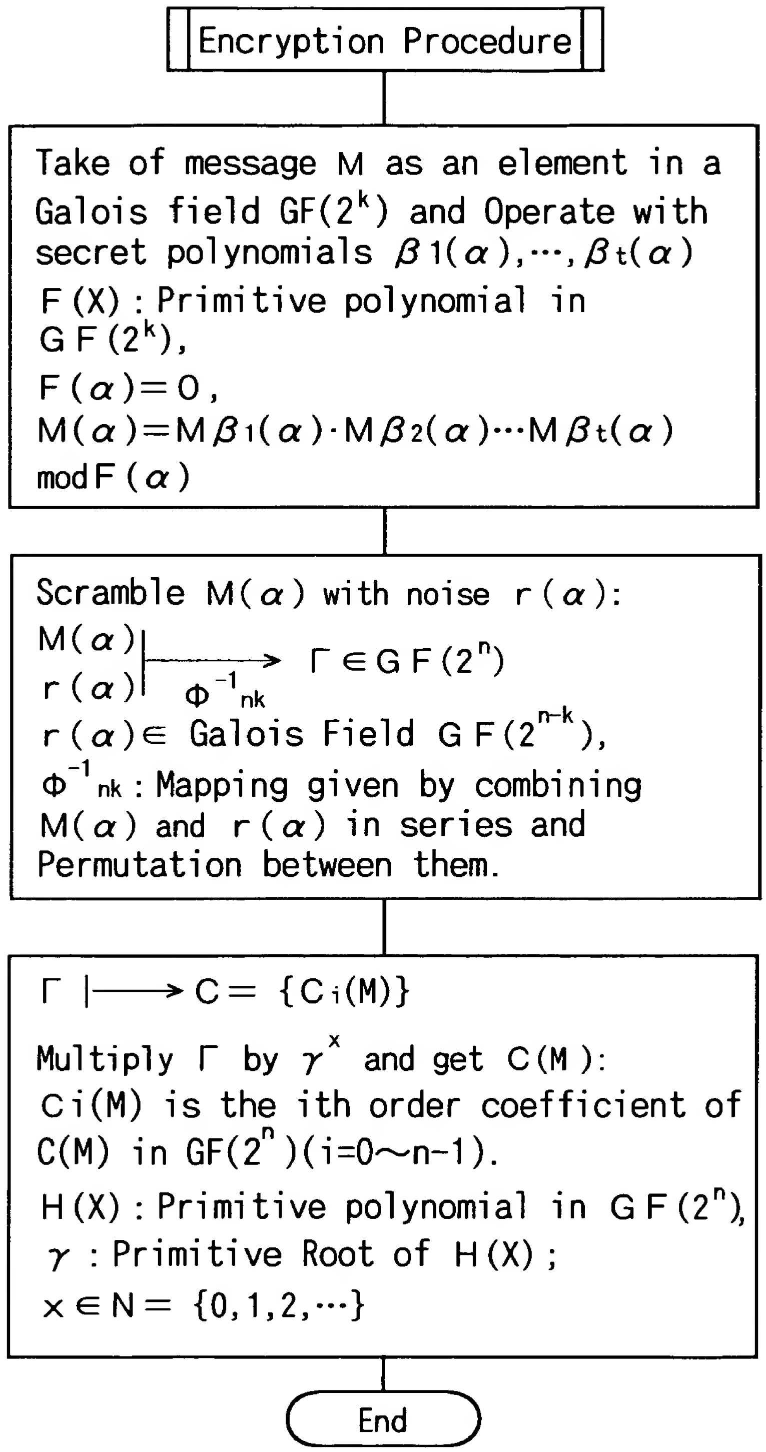
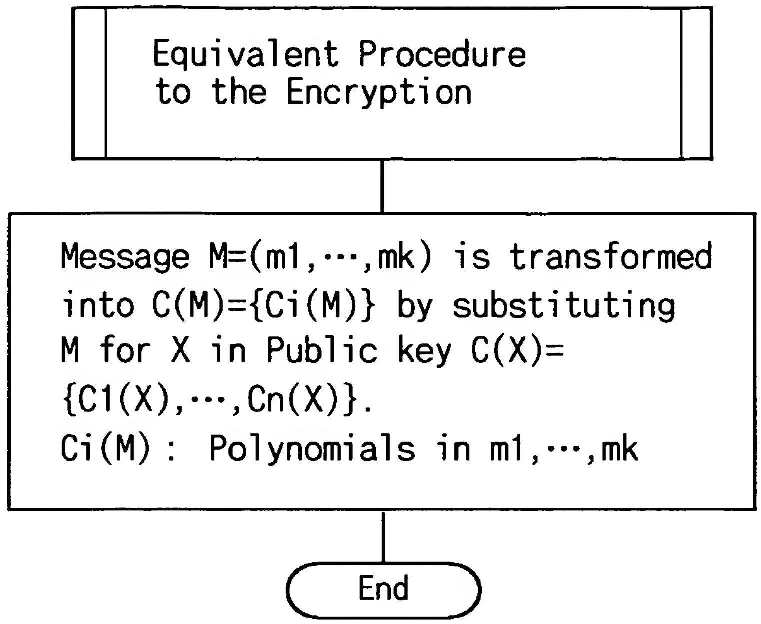

Plaintext Generator
2
Message $M \in GF(2^k)$
$M=(m_1, m_2, \cdots, m_k)$
Encryptor
4
$C(M)=\{C_1(M), C_2(M), \cdots, C_n(M)\}$
$C(M) \in GF(2^n)$
Decryptor
6
$C(M)$
Multiplication
12
$\Gamma=C(M)\cdot\gamma^{-x} \in GF(2^n)$
Permutation
14
$M(\alpha)=\Phi_{nk}\Gamma \in GF(2^k)$
Multiplication
16
$M^t=M(\alpha)\cdot\beta^{-1}$
$M=M^{t\cdot f}$
Public Key
8
$C(X)=\{C_1(X), C_2(X), \cdots, C_n(X)\}$
$F(X), H(X), x, \Phi_{nk}, \beta, t$
10

FIG. 2



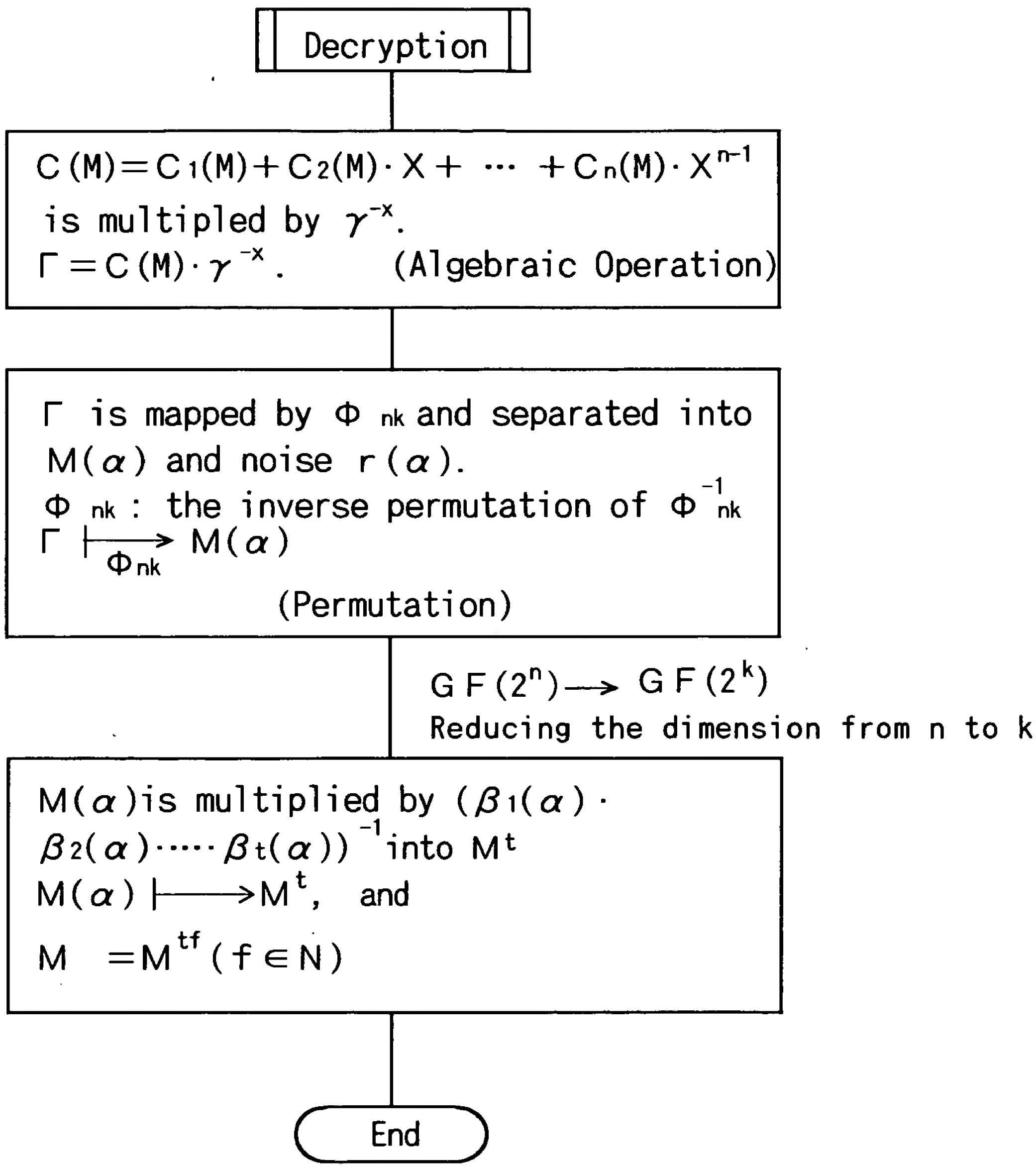
Encryption Procedure
Take of message M as an element in a Galois field $GF(2^k)$ and Operate with secret polynomials $\beta 1(\alpha),\cdots,\beta t(\alpha)$
$F(X)$: Primitive polynomial in $GF(2^k)$,
$F(\alpha)=0$,
$M(\alpha)=M\beta_1(\alpha)\cdot M\beta_2(\alpha)\cdots M\beta_t(\alpha) \bmod F(\alpha)$
Scramble $M(\alpha)$ with noise $r(\alpha)$:
$M(\alpha), r(\alpha) \xmapsto{\Phi^{-1}_{nk}} \Gamma \in GF(2^n)$
$r(\alpha) \in$ Galois Field $GF(2^{n-k})$,
Φ^{-1}_{nk} : Mapping given by combining $M(\alpha)$ and $r(\alpha)$ in series and Permutation between them.
$\Gamma \longmapsto C=\{C_i(M)\}$
Multiply Γ by γ^x and get $C(M)$:
$C_i(M)$ is the ith order coefficient of $C(M)$ in $GF(2^n)(i=0\sim n-1)$.
$H(X)$: Primitive polynomial in $GF(2^n)$,
γ : Primitive Root of $H(X)$;
$x \in N=\{0,1,2,\cdots\}$
End

FIG. 3

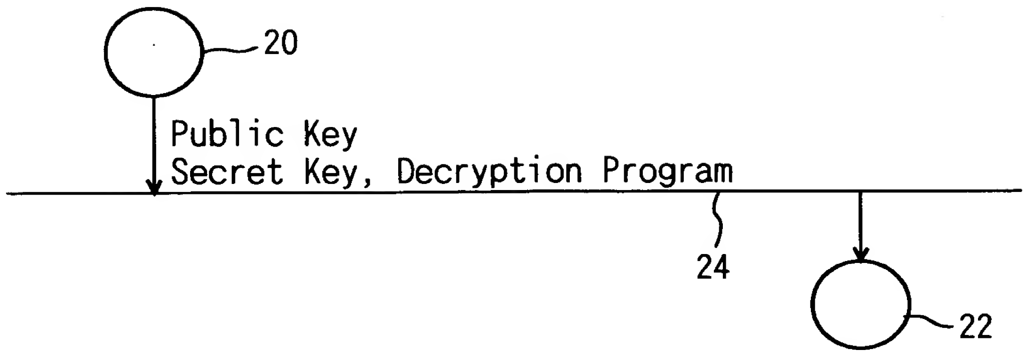


Equivalent Procedure to the Encryption
Message M=(m1,···,mk) is transformed into C(M)={Ci(M)} by substituting M for X in Public key C(X)={C1(X),···,Cn(X)}.
Ci(M) : Polynomials in m1,···,mk
End

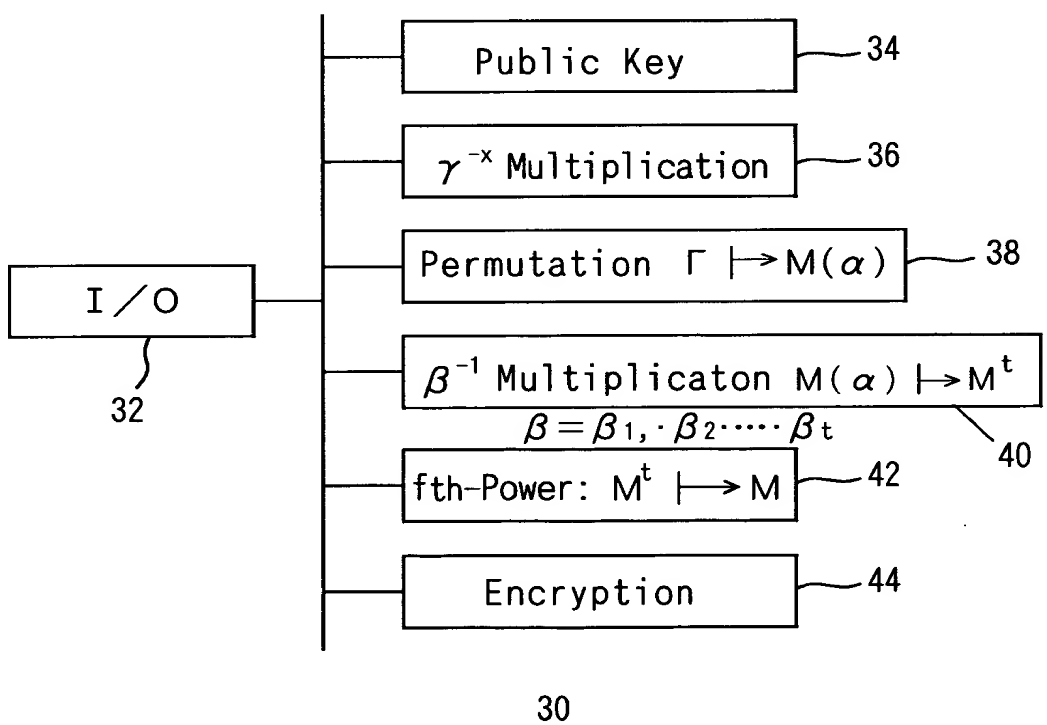
FIG. 4


Decryption
$C(M) = C_1(M) + C_2(M) \cdot X + \cdots + C_n(M) \cdot X^{n-1}$
is multipled by γ^{-x}.
$\Gamma = C(M) \cdot \gamma^{-x}$. (Algebraic Operation)
Γ is mapped by Φ_{nk} and separated into
$M(\alpha)$ and noise $r(\alpha)$.
Φ_{nk} : the inverse permutation of Φ^{-1}_{nk}
$\Gamma \xmapsto{\Phi_{nk}} M(\alpha)$
(Permutation)
$GF(2^n) \longrightarrow GF(2^k)$
Reducing the dimension from n to k
$M(\alpha)$is multiplied by $(\beta_1(\alpha) \cdot \beta_2(\alpha) \cdots \beta_t(\alpha))^{-1}$ into M^t
$M(\alpha) \longmapsto M^t$, and
$M = M^{tf} (f \in N)$
End

F I G. 5


20
Public Key
Secret Key, Decryption Program
24
22

F I G. 6


Public Key
34
γ^{-x} Multiplication
36
Permutation Γ ↦ M(α)
38
I／O
32
β^{-1} Multiplicaton M(α) ↦ M^t
β = β1, · β2 ····· βt
40
fth-Power: M^t ↦ M
42
Encryption
44
30